Н. С. Морозова

ПРОБЛЕМЫ СОВРЕМЕННЫХ СИСТЕМ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ДАННЫХ С КОНЕЧНЫХ ТОЧЕК СЕТИ

Введение

Современный рынок ИТ-решений и услуг предлагает множество продуктов, охватывающих широкий круг задач по защите конфиденциальных данных. Это как одиночные решения конкретных задач, так и комплексные системы, включающие в себя множество функций защиты данных. Относительно новым и популярным на сегодняшний день направлением для российских и зарубежных компаний является разработка и внедрение так называемых DLP-решений (Data Loss Prevention — предотвращение потери данных). Это не единственное, но наиболее распространенное название такого рода систем, предназначенных для минимизации рисков утечек конфиденциальных данных организации. Они перехватывают и анализируют основные информационные потоки (каналы утечек) данных, которые пересекают периметр защищаемой (корпоративной) сети, тем самым позволяя своевременно выявлять несанкционированные действия с конфиденциальной информацией, пресекать такие действия, помогают в сборе доказательств и расследовании инцидентов ИБ [1].

Появление DLP-систем и их нынешняя популярность напрямую связаны с возросшей в них необходимостью. По данным отчета Securit Analytics об утечках информации, за 2010 г. зафиксировано 1014 утечек, что на 15,6 % больше показателя 2009 г., каждый рабочий день 2010 г. происходило в среднем 4 утечки. Лидером по числу инцидентов являются США, на их долю приходится 88,4 % всех случаев. На долю России приходится всего 3,5 %, но общее количество инцидентов (37) на 60,9 % больше, чем в 2009 г. Средний ущерб от одной утечки в 2010 г. составил $ 3793726, что на 49,3% ниже показателей 2009 г., но сумма все же пугающая. Вследствие этого страдает не только репутация организаций, их и государственный бюджет, но и люди, поскольку основной долей утекающих данных (63,6 %) были персональные данные сотрудников и клиентов. Не стоит забывать и о том, что приведенные цифры относятся лишь к официально обнародованной информации об инцидентах, связанных с утечками данных, число которых, по оценке Securit Analytics, составляет в лучшем случае 0,1 % от числа всех инцидентов [2].

Обширное внедрение и использование DLP-систем должно улучшить эту статистику. Но их повсеместному внедрению препятствуют несколько проблем. Во-первых, высокая стоимость DLP-систем делает их доступными лишь небольшому кругу крупных компаний, во-вторых, их внедрение и использование требуют немалых трудозатрат. В-третьих, богатый функционал и высокий уровень развития современных решений класса DLP позволяют выявлять и предотвращать несанкционированные действия с различными видами конфиденциальных данных, но не существует методики оценки DLP-систем, которая показала бы зависимости уменьшения рисков утечки и защищенности информационной системы от внедрения решения и от корректности его настроек. Также довольно сложно привести экономическое обоснование для внедрения и использования такой системы даже в крупной компании. Эти трудности и проблемы будут подробнее описаны позже.

Сегодня на российском рынке DLP-систем присутствуют как известные мировые вендоры (Symantec, Websense, TrendMicro, McAffee), так и отечественные производители (InfoWatch, «Инфосистемы Джет», SearchInform, SecureIT и другие). Аналитические обзоры [3] и [4] российского рынка DLP-систем приводят объемы продаж и долей рынка основных представителей, а также описывают некоторые особенности предлагаемых ими систем. К числу ведущих представителей можно отнести российские компании InfoWatch и «Инфосистемы

Джет» [3] и одного из мировых лидеров — компанию Symantec, которая первой представила пакет локализации для России своего DLP-решения Russian Language Pack for Symantec DLP в середине 2010 г. [5].

Как правило, комплексные DLP-системы включают в себя три основные подсистемы [6]:
- сетевую подсистему (Network DLP) — для защиты конфиденциальных данных, передаваемых по электронной почте и различным веб-протоколам;
- подсистему для защиты конечных точек сети (Endpoint DLP) — для защиты конфиденциальных данных на рабочих станциях, копируемых на внешние устройства и носители, отправляемых на печать;
- подсистему для защиты статических данных (Content Discovery) — для обнаружения и защиты конфиденциальных данных, хранимых в различных файловых хранилищах, базах данных.

Достаточно долгое время на российском рынке подавляющее большинство решений класса DLP представляли собой системы контроля сетевого трафика, поэтому именно сетевая подсистема многих современных DLP-систем наиболее развита и отлажена. Сегодня существуют не только программные реализации таких подсистем, но и шлюзы с интегрированным в них функционалом сетевых DLP. Очевидная потребность в защите от утечек конфиденциальных данных, копируемых на внешние устройства и носители, отправляемых на печать, обусловила большой темп развития подсистем DLP для защиты рабочих станций. Сегодня такие подсистемы имеют большой набор функций и позволяют контролировать информационный обмен рабочей станции пользователя с широким кругом портативных устройств (Device Control). Также многие подсистемы позволяют контролировать данные, передаваемые различным приложениям на рабочей станции пользователя (Application Control). В рамках статьи автором рассматриваются функции подсистем DLP по контролю использования портативных устройств и внешних носителей, далее — DLP КВНУ (контроль внешних носителей и устройств).

Функции DLP КВНУ

Все DLP-системы функционируют на основе центральной политики [7], для DLP КВНУ настройки политик могут быть как в отдельной консоли управления, так и в рамках единой для всей системы консоли управления (это лишь вопрос конкретной реализации). Все функции, реализованные в DLP КВНУ, имеют соответствующие им пункты настроек в консоли управления.

Конечно же, основной функцией любой DLP КВНУ является контроль доступа пользователя к различным устройствам и портам ввода-вывода. По этой позиции все решения отличаются лишь списком поддерживаемых устройств и портов. Основной набор устройств: дисководы, CD/DVD-приводы, съемные накопители, жесткие диски, КПК (карманные персональные компьютеры) и смартфоны, локальные и сетевые принтеры, Wi-Fi и Bluetooth передатчики и другие; порты USB, FireWire, COM, LPT, IrDA. Зато относительно глубины контроля, применимости основных и наличия дополнительных функций для конкретных типов устройств решения могут достаточно сильно различаться.

Под глубиной контроля в данном случае подразумевается возможность задания прав доступа и реализации других функций системы на следующих уровнях:
- для класса устройств;
- для конкретного устройства (зависит от наличия возможности идентификации устройств по тем или иным параметрам);
- для файлов определенного типа и/или расширения.

Следующей основной функцией DLP КВНУ является теневое копирование файлов, записываемых на внешние устройства и носители и/или копируемых с них на рабочую станцию пользователя. Эта функция может поддерживаться не для всех типов устройств и, может быть, не

для всех типов данных. Например, в случае смартфонов и КПК может поддерживаться теневое копирование файлов приложений, текстовых фалов и мультимедиа-файлов, а файлов с данными календаря, контактов, заметок и т. п. — нет.

Многие DLP КВНУ предоставляют возможность идентифицировать некоторые устройства по их уникальному идентификатору, например флеш-карты, внешние жесткие диски и другие съемные устройства. Некоторые также предоставляют возможность идентификации CD/DVD-дисков на основе записанных на них данных. Таким образом, возможно, например, зарегистрировать в системе корпоративные съемные накопители и разрешать доступ только к ним, а также выявлять случаи подключения и использования незарегистрированных (личных) накопителей.

Функциональные возможности DLP КВНУ по настройке политик также могут различаться, но основными для большинства систем являются следующие:

- политика применяется к рабочей станции или ноутбуку, которые могут быть объединены в группы (права для каждого компьютера вычисляются исходя из глобальной политики (при ее наличии), групповой и «точечной» политик; как правило, в документации к системе должны быть описаны правила вычисления или представлены матрицы прав доступа);
- права назначаются для пользователей или групп пользователей (интеграция с Active Directory);
- существует разделение прав на чтение и запись (для некоторых систем также задается степень приоритета, который учитывается при вычислении результирующих прав доступа);
- возможность применения разных наборов политик в зависимости от наличия сетевого подключения рабочей станции или ноутбука к корпоративной сети (некоторые решения предоставляют возможность использования различных политик в зависимости от дня недели и времени);
- возможность экспорта (и последующего импорта на рабочей станции) файла настроек политик, которая может использоваться для обновления политик на рабочей станции, не имеющей подключения к корпоративной сети.

Также некоторые системы предоставляют возможность использования специальных политик для зашифрованных накопителей. Причем система может быть интегрирована со сторонними средствами шифрования, а также иметь собственные (встроенные) средства.

Возможность отдельной настройки политик при отсутствии подключения к корпоративной сети важна для защиты данных, хранимых на ноутбуках пользователей. Например, можно запретить копирование конфиденциальной информации на внешние носители, тем самым снизив возможность утечки таких данных, когда ноутбук находится за пределами стен компании.

Практически все DLP КВНУ имеют возможность формирования различных отчетов, а также хранят журналы аудита и теневого копирования. Сегодня многие системы включают в себя возможность формирования множества детализированных, а также графических отчетов различного назначения, начиная от статистики использования тех или иных устройств и заканчивая сложными аналитическими отчетами, основанными в том числе и на содержимом файлов теневого копирования.

Ядром современных DLP-систем является реализованная в них технология категоризации информации [8], которая используется для анализа данных всеми подсистемами DLP-решения. Именно она является основой для глубокого анализа данных и принятия решения о возможности копирования информации на внешние устройства в случае DLP КВНУ. Учитывая только описанные выше функции, возможно либо разрешить (чтение и/или запись), либо запретить использование устройств и копирование определенных типов файлов. Это противоречит *основному подходу* к защите конфиденциальных данных с использованием DLP-систем — нельзя полностью исключить доступ, но необходимо защищать конфиденциальные данные и минимально ограничивать действия пользователей, т. е. блокировать только те действия, которые могут принести вред [7]. Этот подход важен для нормального функционирования бизнес-процессов.

Встроенные механизмы лингвистического анализа и статистических методов детектирования конфиденциальных данных позволяют ограничивать действия (настраивать политики) исходя из содержимого копируемых файлов.

Многие DLP-системы предоставляют возможность анализа данных, используя:

- словари терминов;
- регулярные выражения;
- контекстный анализ;
- семантический анализ;
- цифровые отпечатки документов и баз данных;
- шаблоны документов.

Чаще всего во многих системах уже существует набор готовых правил для обнаружения, например, паспортных данных, номеров кредитных карт, стандартных форм бухгалтерской или финансовой отчетности. Также имеется словарь терминов, по наличию которых информацию можно классифицировать по функциональной принадлежности: финансовая, маркетинговая, юридическая и т. д. [8].

В этой нише разработчики DLP-систем борются за число поддерживаемых их модулем анализа данных форматов файлов, кодировок, методов анализа, а также за наличие отличительных дополнительных функций.

Хотелось бы отметить, что некоторые системы дают возможность полнотекстового поиска по содержимому файлов теневого копирования. Эта функция может быть очень полезна не только для сбора доказательств при расследовании ИБ-инцидентов, но и для того, чтобы при необходимости среди множества документов найти тот, который отвечает определенным критериям, например не подходящий под имеющиеся в механизме категоризации данных настройки.

Также как полезную функцию можно рассматривать уведомления пользователя о запрете копирования документа, в содержании которого была обнаружена конфиденциальная информация, например, на флеш-карту. Такие уведомления способствуют обучению пользователей правилам работы с конфиденциальной информацией или лишний раз напоминают, что подобные действия запрещены.

Таким образом, современные DLP КВНУ обладают комплексом функций для предотвращения утечки конфиденциальных данных с рабочих станций и ноутбуков пользователей посредством внешних носителей и портативных устройств, а также имеют возможности гибкой и детализированной настройки политик защиты. Но все эти возможности порой перекрываются трудностями, возникающими при внедрении и эксплуатации DLP-решения.

Трудности внедрения и использования DLP-систем

Несмотря на огромные возможности, далеко не все внедренные решения работают в полную силу. На этапе внедрения производятся настройка и отладка правил и политик для защиты ограниченного набора конфиденциальных данных организации. Для крупномасштабного внедрения требуется произвести инвентаризацию и классификацию всей конфиденциальной информации компании [9], что является трудновыполнимой задачей для небольшой компании, а для крупной — представляется невыполнимым. Поэтому ряд организаций, столкнувшись с данной проблемой, оставляют первоначальные (отлаженные) правила и политики, которые, с одной стороны, со временем устаревают, а с другой — не охватывают весь объем циркулирующей в компании информации. Результат от работы системы в таком (первоначальном) режиме, конечно, есть, поскольку, как отмечалось ранее, многие DLP-системы уже содержат в себе основные правила для защиты некоторых персональных данных, данных счетов и кредитных карт и другие. В дополнение к этому при внедрении для отладки системы могут использоваться наиболее критичные данные и бизнес-процессы компании.

Одним из путей решения описанной проблемы является интеграция DLP-систем с другими системами, такими как: управление правами на документы (Enterprise Digital Rights Management), сбор и анализ событий безопасности и управление инцидентами, системы электронного документооборота и др. [9]. Другим путем является развитие разработчиками подсистемы обнаружения и защиты конфиденциальных данных (Content Discovery) и внедрение ее в DLP КВНУ. Такая подсистема сканирует места хранения данных, выявляет конфиденциальные данные и на основе заданных политик проверяет правильность условий хранения таких данных.

Другой сложной и трудоемкой задачей при использовании DLP-систем является настройка правил анализа данных и пополнение словарей терминов. Необходимость в совершении таких действий может быть обусловлена несколькими причинами: добавление новых категорий конфиденциальной информации, поддержание актуальности настроек системы, улучшение качества настройки системы. Улучшение качества настроек является сложным процессом, вызванным большим числом ложных срабатываний системы. Если настройкой системы не удается уменьшить число ложных срабатываний, то стоит задуматься о качестве самой системы и ее применимости в данных конкретных условиях [10].

Настройка правил и политик и введение новых терминов для новой категории конфиденциальной информации тоже представляет собой непростую задачу, особенно для крупной организации. Во-первых, для выделения новой категории и подготовки соответствующих терминов даже специалисту в своей области может понадобиться помощь лингвиста. Во-вторых, поскольку все настройки выполняются в консоли управления системой сотрудником информационной безопасности (техническим специалистом), то требуется его тесное взаимодействие с ответственным за данную информацию сотрудником на этапах составления правил и их отладки. Для крупных и/или территориально распределенных компаний такое взаимодействие порой бывает затруднительным, также технические специалисты и представители других, гуманитарных, профессий нередко не понимают друг друга (говорят на «разных» языках). Дополнительно необходимо учитывать непротиворечивость новых правил с уже имеющимися в системе. Как следствие, некорректная настройка и/или противоречивость правил приводит к увеличению числа ложных срабатываний системы и, возможно, «пропуску» системой некоторых конфиденциальных данных.

Необходимо учитывать возможность возникновения следующих трудностей и проблем.

Программные решения зарубежных поставщиков, порой очень успешные, не всегда применимы в российских компаниях. Это связано в первую очередь с отсутствием локализации системы, в частности ее модуля анализа информации. Для поддержки того или иного языка недостаточно добавить словарь и кодировки — требуется изменение алгоритмов анализа, поскольку правила словообразования у разных языков разные. Эту особенность необходимо также учитывать и при необходимости поддержки системой, даже от российских разработчиков, дополнительных языков, например украинского.

Многие производители заявляют о поддержке огромного множества форматов обрабатываемых их системой файлов. Это в первую очередь относится к теневому копированию и отображению содержимого этих файлов в системе, а анализу часто подвергаются лишь текстовые документы. Также порой не все из заявленных форматов файлов корректно разбираются и анализируются. Поэтому необходимо тщательно подходить к вопросу тестирования системы (подготовки тестовых данных).

В связи с этим отметим, что некоторые системы не только позволяют анализировать текстовую информацию, но и содержат функцию распознавания текстов (интегрированы с соответствующими программными продуктами или имеют встроенный модуль) с их последующим анализом. Также некоторые системы анализируют не только содержимое файлов, но и атрибуты файлов, что нередко помогает в создании правил категоризации файлов (например, все файлы, созданные генеральным директором, конфиденциальны).

Следует еще раз отметить высокую стоимость DLP-решений, которая порой соизмерима с суммарной стоимостью всех используемых организацией средств защиты. Поэтому целесообразность использования таких мощных и дорогостоящих систем малыми и средними компаниями редко бывает оправдана.

Для крупных организаций помимо очевидно развитого функционала современных DLP-решений важна возможность интеграции DLP-решения с другими корпоративными системами. Здесь могут быть свои сложности, такие как несовместимость версий программных продуктов (нередко в крупной компании обновление версии программного обеспечения растягивается на достаточно большой период времени), совместимость DLP-решения с системами компании, разработанными и сопровождаемыми самостоятельно.

Заключение

Современные DLP-системы являются комплексными продуктами с множеством функций для защиты конфиденциальных данных организации от их утечки по различным каналам, включая внешние накопители и портативные устройства. Подавляющее большинство решений ориентировано на внедрение в крупные организации, но их полноценное использование возможно лишь после преодоления всех трудностей, начиная от очевидных сложностей при выборе решения конкретного разработчика и заканчивая отмеченными выше проблемами при внедрении и эксплуатации DLP-систем.

СПИСОК ЛИТЕРАТУРЫ:

1. *Васильев В.* DLP-системы на этапе перевода ИТ на облачную платформу // PC Week Review: ИТ-безопасность. 2011. № 3. С. 14–16.
2. Отчет об утечках корпоративной информации и персональных данных за 2010 год // Securit Analytics. URL: http://www.secureit.ru/docs/secureit_research_2010.pdf.
3. *Шабанов И., Ренселаева К.* Анализ рынка систем защиты от утечек конфиденциальных данных (DLP) в России 2009–2011 // Anti-Malware: информационно-аналитический центр. URL: http://www.anti-malware.ru/russian_dlp_market_2009_2011.
4. Основные игроки российского рынка DLP // Банкир.Ру. URL: http://www.bankir.ru/technologii/s/osnovnie-igroki-rossiiskogo-rinka-dlp-9862829.
5. Symantec DLP — первая в мире DLP-система на русском языке среди лидеров рынка // Symantec Corporation. URL: http://www.symantec.com/ru/ru/about/news/release/article.jsp?prid=20100901_01.
6. *Kanagasingham P.* Data Loss Prevention // SANS Institute InfoSec Reading Room. URL: http://www.sans.org/reading_room/dlp/data-loss-prevention_32883.
7. *Mogul R.* Best Practices for Endpoint DLP // Securosis: Information security Research & Analysis. URL: http://www.securosis.com/publications/BestPracticesforEndpointDLP.pdf.
8. *Хайретдинов Р.* Как работают DLP-системы? // Хакер. 2011. № 3. С. 118–121.
9. DLP системы // Leta IT Company. URL: http://www.leta.ru/library/analytics/inside-015/inside-015.html.
10. *Федоров Н.* Возможные метрики ИБ при выборе и использовании DLP-систем // PC Week Review: ИТ-безопасность. 2011. № 3. С. 16.